DEPARTMENT OF THE NAVY
COMMANDER NAVY REGION SOUTHWEST
937 NO. HARBOR DR.
SAN DIEGO, CALIFORNIA 92132-0058

IN REPLY REFER TO:

COMNAVREGSWINST 2280.1A
N6

DEC 0 1 2004

COMNAVREGSWINST 2280.1A

Subj: GUIDANCE FOR ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) PROCEDURES

Ref: (a) EKMS 1
(b) SECNAVINST 5510.36
(c) SECNAVINST 5510.30A
(d) OPNAVINST 5530.14C
(e) CMS 5

Encl: (1) Authorization to Receipt for and Courier COMSEC Material
(2) STU-III CIK Data Log, Sample
(3) Data Transfer Device (DTD) Audit Trail Review Log, Sample

1. Purpose. To promulgate procedures for the establishment and maintenance of Local Element (LE) accounts as defined in reference (a) and as they pertain to Commander, Navy Region Southwest EKMS parent account. Throughout this instruction the use of the term "EKMS" will apply to electronically generated keying material, traditional Communications Security (COMSEC) material, Controlled Cryptographic Items (CCI), Secure Telephone Unit Third Generation (STU-III), Secure Terminal Equipment (STE), and Future Narrowband Digital Terminal (FNBDT) material.

2. Cancellation. COMNAVREGSWINST 2280.1

3. Scope. This instruction gives specific guidance to LE accounts of CNRSW EKMS account. References (a) through (e) will take precedence in any area of contradiction. Enclosures (1) through (3) are provided to assist in the management and administration of LE EKMS accounts. The EKMS Parent Account Manager for Commander, Navy Region Southwest will be contacted immediately to resolve any discrepancies.

4. Background

a. EKMS is an interoperable collection of systems developed by services and agencies of the U.S. Government to automate the planning, ordering, generating, distributing, storing, filling, use, and destruction of electronic key and management of other types of COMSEC material. The EKMS provides for the security of highly sensitive and classified communications material and related devices. Because of the

extreme sensitive nature of EKMS material, a continuous chain of custody receipts, positive accounting records, and immediate reporting of loss, compromise, or possible compromise is required from the time of its entry into the system until it is destroyed.

b. Management and security of EKMS material are inherent responsibilities at all levels of command. Proper evaluation of EKMS administrative procedures can be made only if all officers in the chain of command are knowledgeable and support compliance with established EKMS procedures and requirements. It is necessary therefore, that officers senior to the EKMS Manager and/or LE EKMS personnel be familiar with, and participate in the management of EKMS material.

c. Reference (a) establishes guidelines and general procedures for operation and maintenance of EKMS accounts. Reference (b) is the Navy "Information Security Program," reference (c) is the Navy "Personnel Security Manual," reference (d) is the Navy "Physical Security Manual," and reference (e) provides information related to CCI support and procedures.

d. Under the EKMS system, CNRSW is the EKMS Parent Account and entities, units, or commands, internal or external, which require COMSEC support from Navy Region Southwest, are considered Local Elements. The EKMS Parent Account is maintained at Naval Base Coronado, North Island complex, Building 318, Room 118.

5. Action.

a. Commanders, Commanding Officers, Staff CMS Responsibility Officers, and Officers-in-Charge of Local Elements will:

(1) Designate a Custodian and at least two alternates or users in writing to administer the LE EKMS account. Each individual must meet the designation requirements in Article 420 of reference (a). A copy of each designation letter must be forwarded to the CNRSW EKMS Manager.

(2) Ensure at least two individuals, as designated above, are available at all times in case of emergencies.

(3) Designate personnel in writing authorized to use EKMS keying material to accomplish assigned duties. This designation may be an individual letter or take the form of a command letter listing all Users. If an individual letter is used, it remains in effect until the status of the individual

changes. If an access list is used, it must be updated whenever the status of an individual changes or at least annually.

(4) Per Annex I of reference (a), submit a letter or message designating personnel authorized to draw and courier classified EKMS material from the parent account. Ensure the letter is addressed to COMNAVREG SOUTHWEST and not CMIO. All individuals designated must possess a clearance equal to or greater than the highest security level handled. Enclosure (1) is a sample letter with the minimum required information. This information must be updated annually or whenever there is a change in the custodian or alternate(s) status.

(5) Ensure the command Immediate Superior In Command (ISIC) certifies in writing the spaces used for handling and storage of EKMS material up to and including the classification of the EKMS material assigned to your command.

b. Any command requiring EKMS support from CNRSW may be designated as LE by the execution of a letter of agreement (reference (a), Annex L). LE commands must provide the parent account with written acknowledgement indicating receipt and concurrence with the agreement when initially designated and upon change of command by either the LE command or the parent account command. Letters of agreement will be reviewed annually and revised as necessary.

6. Responsibilities of EKMS Personnel

a. EKMS Manager. An individual designated in writing by the Commanding Officer to manage EKMS material issued to the EKMS account. The EKMS Manager is the Commanding Officer's primary advisor on matters concerning the security and handling of EKMS material and the associated records, reports, and audits. The EKMS Manager must meet all the designation requirements of reference (a), Article 415. The duties and responsibilities of the EKMS Manager are delineated in reference (a), Article 455. The EKMS Manager shall ensure that Alternate Managers, Users, Witnesses and Clerks understand their responsibilities and ensure they are sufficiently trained to carry out their duties. The EKMS Manager shall monitor the overall internal security, accountability, control, storage, storage facilities and disposition of EKMS material, and provide oral and written guidance to all command personnel who use EKMS material. The EKMS Manager shall review command directives at least annually to ensure their continued accuracy.

b. Alternate Manager(s). Alternate Manager(s) share joint responsibility with the EKMS Manager to the Commanding

Officer for proper management and security of all EKMS material held by the command. As such, the Alternate EKMS Manager(s) has the same duties and responsibilities as an EKMS Manager. The Alternate Manager(s) must be actively involved in the daily operation of the account and be ready at all times to fully administer the account in the absence of the EKMS Manager. The Commanding Officer has full authority to waive the normal requirement for two Alternate Managers and may appoint more or less, **but in no case** fewer than one alternate is authorized. All waivers must be addressed to the parent account, with information copy to the command ISIC, and retained on file until no longer effective.

c. Local Elements (LE). Local Elements are separate entities, units, or commands (internal or external to the EKMS parent account) who require EKMS support. External LEs, formerly called "Local Holders," report to a Commanding Officer other than the parent account. Internal LEs formerly called "Users," report to the same Commanding Officer as the parent account. Under the EKMS system, LE Custodians are now called "Local Element Issuing" and the LE Users are called "Local Element Using." LE Issuing must be designated in writing by the Commanding Officer and meet the designation requirements of reference (a), Article 420. LE Issuing duties and responsibilities are delineated in reference (a), Article 465.

d. Witness. Any properly cleared U.S. Government employee (military or civilian) who may be called upon to assist a Custodian or User in performing routine administrative tasks related to the handling of EKMS material. A witness must be formally authorized access to EKMS keying material. The duties and responsibilities of a Witness are delineated in reference (a), Article 480. The Witness must meet all the designation requirements of reference (a), Article 420.

e. Account Clerk. An individual designated in writing by the Commanding Officer who assists the manager and Alternate(s) with routine administrative account matters. This designation is at the discretion of the Commanding Officer. The Account Clerk is authorized access to EKMS material, and may assist management personnel maintain Two-Person Integrity (TPI). Account Clerks can sign receipt, inventory, and destruction reports as a witness only. An Account Clerk is not authorized to have knowledge of or access to security container combinations.

7. Training. The EKMS Manager, Alternate Manager(s), and/or designated LE Issuing personnel shall conduct training in the

proper receipt, distribution, handling, storage, inventory, and disposition of EKMS material to LEs, Witnesses, Clerks, and other personnel who participate in the management of such material. Particular attention should be given to identifying improper practices. They should, at a minimum, use classroom instruction, require reading of appropriate EKMS publications and documents, provide on the-job training, and perform spot checks to ensure training goals are met. Training should be conducted on a monthly basis and documented using a standard muster sheet with the topic, instructor's name, date of training, and signatures of personnel attending. A copy of the training sheet will be forwarded to the parent EKMS Manager.

a. The Local Holder (LH) Computer Based Training (CBT) Course (V-4C-0031) provides personnel the basic skills necessary to fill an LE Issuing position. The LH CBT is an Interactive Courseware (ICW) CBT CD-ROM that emphasizes management of an EKMS LE account and operation of the data transfer device (DTD). LE Issuing personnel must complete the LH CBT within 30 days after appointment. The course may be obtained from the Parent EKMS Account Manager.

b. Military personnel (except USMC/USCG) must complete the CMS Personnel Qualification Standard (PQS) (NAVEDTRA 43462 (series)) FSN 0501-LP-478-5600 no later than six months after appointment as Manager or LH Issuing. All military and civilian personnel that have not previously completed the Navy PQS will be required to complete the CNRSW EKMS Job Qualification Requirements (JQR) prior to handling COMSEC material. New LE Issuing and Using personnel shall obtain a copy of the CNRSW EKMS JQR from the EKMS Manager.

c. The CMS Advice and Assistance (A&A) Team provides several very helpful EKMS training programs for Local Elements. "CMS for Commanding Officers," "Local Element Account Training," "Data Transfer Device (DTD) Training", and "STU-III Briefs" are just a few of the many programs offered. These courses provide guidance on the policy and procedures for handling EKMS material.

8. Access and Safeguarding. EKMS material, including STU-III seed keys and crypto ignition keys (CIK), must be in the direct and continuous control of authorized persons. When not in use, EKMS material must be stored in approved locked storage containers. Storage containers (e.g., vaults, strong rooms, safes) used to safeguard EKMS material shall provide maximum protection against unauthorized access, damage, sabotage, and deterioration.

a. EKMS material and files will be stored per their assigned classification. Classified material storage requirements are outlined in Chapter 7 of reference (b).

b. Access to EKMS material shall be granted only to those persons who have written authorization, a valid need-to-know, possess the appropriate security clearance, and have completed a COMSEC Responsibility Acknowledgement Form found in Annex J of reference (a). They must also have been properly indoctrinated regarding the sensitivity of the material, the rules for safeguarding such material, and the laws pertaining to espionage. Access to unkeyed CCI material does not require a security clearance; however, access must be restricted to U.S. citizens whose duties require such access.

c. Two-Person Integrity (TPI) Requirements. TPI is a system of handling and storage designed to prevent single-person access to certain EKMS material. TPI must be applied to all TOP SECRET keying material marked or designated CRYPTO. It also applies to fill devices (FDs) or other physical media (floppy disk, magnetic tape, etc.) storing unencrypted TOP SECRET key, and electronic key whenever it is generated, transferred (OTAR/OTAT), relayed or received (OTAT) in an unencrypted form. Equipment containing TOP SECRET key that allows for extraction of the loaded key, as well as unloaded FDs in an operational environment containing such equipment, requires TPI.

(1) TPI handling requires at least two appropriately cleared persons authorized access to EKMS keying material be in constant view of each other and the EKMS material requiring TPI whenever the material is accessed and handled. This includes removing unencrypted TOP SECRET key marked or designated CRYPTO from equipment, key variable generators (KG-83), and whenever TOP SECRET key is generated using a key variable generator. Each person must be capable of detecting incorrect or unauthorized security procedures with respect to the task being performed. When TPI material is not being handled, it must be locked in a TPI-approved security container as specified in reference (a), Article 520.

(2) TPI storage requires the use of two approved combination locks (each with a different combination) with no one person having access to or knowledge of both combinations. TPI storage may also be maintained by the use of a General Services Administration (GSA) procured security container or vault door equipped with combination locks meeting Federal Specification FF-L-2740. Per reference (b), Article 10-3b, SECNAV set a mandatory date of **1 October 2002**, for replacing all classified material containers with GSA-approved containers.

(3) Exceptions to TPI Requirements:

(a) Mobile users: USMC tactical units, Naval Special Warfare (SPECWAR) units, Naval Construction Battalion (NCB) units, Explosive Ordnance Disposal (EOD) units, Mobile Inshore Undersea Warfare units (MIUWUs), and other similar mobile users are exempt from EKMS key TPI requirements only while operating in a tactical exercise or operations field environment.

(b) Aircraft: TPI is not required for FDs during the actual loading process in the aircraft; however, TPI is required on loaded FDs, which contain unencrypted TOP SECRET key up to the flight line boundary. Loaded FDs placed in an Aircrew COMM box locked with TPI-approved combination locks fulfill TPI requirements. Consequently, one Aircrew member may transport the locked COMM box up to the flight line boundary. Loaded FDs may be stored on board the aircraft in a single-lock container while the aircraft is in a flight status.

(c) Keying material marked SECRET and/or below does not require TPI, regardless of CRYPTO markings.

(d) Facilities/spaces are to be used solely for the storage of unkeyed equipment.

9. Combinations Protecting EKMS Material: Only properly cleared and authorized individuals may have knowledge of and access to combinations protecting EKMS material. Except in an emergency, only the EKMS Manager and Alternate(s) shall have the combinations to the EKMS vault or safe(s). No one manager will have access to or knowledge of both TPI combinations. Accordingly, only LE Issuing personnel may have access to or knowledge of the LE account vault and/or safe(s) combinations.

a. Combinations must be changed when the lock is initially placed in use, when persons having knowledge of the combination no longer require access, when the combination is compromised or suspected to be compromised, when the combination is taken out of service, or at least once every two years.

b. Combinations protecting EKMS material and personal identification numbers (PINs) used with key generating equipment (e.g., KG 83, KOK 22A, etc.) shall be recorded individually and sealed per guidance in reference (a), Article 515f. It is specifically **prohibited** for an individual to record, carry, or store combinations and PINs insecurely for

personal convenience. This includes storing combinations in electronic form in a computer, calculator, personal data assistant (PDA), or similar electronic device.

10. Records and Files. LEs issuing EKMS keying material and/or equipment shall maintain a Chronological File, Correspondence File, General Message File, and a Local Custody File.

a. The Chronological file will contain SF 153 accounting reports (receipts and transfers between LE and parent account, etc.), Accountable Item Summary (formally called Running Inventory), authorization letters to receipt and courier COMSEC material from parent account, and COMSEC Responsibility Acknowledgement forms.

b. The Correspondence file will contain account registration correspondence, Appointment letters, EKMS incident, PDS reports, command allowance correspondence, authorization letters to store classified EKMS material, assist visit and inspection correspondence, and a list of command personnel authorized access to EKMS keying material. This file will also contain a copy of each effective directive of the command and higher authority, which relates to EKMS matters, and waivers of EKMS policy and procedures.

c. The General Message file will contain a copy of each ALCOM and ALCOMPAC "P" message concerning EKMS and affecting the LE command. It is not necessary to maintain copies of messages that do not affect the command; however, a log must be kept for each general message file in order to know whether potentially important messages are missing.

d. The Local Custody file will contain current signed local custody documents reflecting the issue of EKMS material to LE users. There must be a signed document for all EKMS material not under the direct and continuous control of the LE Issuing and/or Alternate(s).

e. Additionally, LEs shall maintain copies of applicable manuals, publications, and directives listed in Article 721 of reference (a). Consult the EKMS Manager for guidance.

f. LEs who only have STU-III terminals and seed keys shall maintain a Local Custody file, CIK Data Log, and Correspondence file consisting of appointment letters, authorization letters to receipt and courier COMSEC material from parent account, STU-III User Responsibility Acknowledgement forms, and authorization to store and use classified STU-III material. (Enclosure (2) is an example of a filled in CIK Log.)

11. Storage Requirements. The ultimate effectiveness and protection provided by EKMS material, systems, equipment, and techniques are dependent upon the actions of each individual EKMS material user. The security achieved through the proper use of crypto systems is also dependent upon the physical protection and storage facilities afforded the associated keying material.

a. LEs shall store EKMS material only in containers and spaces approved for their storage. Where necessary, they shall comply with supplementary controls (e.g., guards and alarms) for safeguarding classified material per Chapter 7 of reference (b). Unless EKMS material is under the direct and continuous control of authorized persons, the material must be kept in locked containers.

b. EKMS material must be stored separately from other classified and non-EKMS material, e.g., in separate containers or in separate drawers.

c. Unless absolutely necessary, do not place EKMS material containers in commonly used spaces where access cannot be controlled. During non-working hours, security containers should be located in locked areas not accessible to general traffic.

d. A Classified Container Information Form (Standard Form 700 (8-85)) for each lock combination must be placed on the inside of each EKMS storage container.

e. A security container open/closure log (Standard Form 702) must be maintained for each lock on an EKMS storage container. If a combination lock meeting Federal Specifications FF-L-2740 (e.g., Mas-Hamilton X-07, X08 or X-09) is used to maintain TPI, an SF 702 will be used for each combination.

f. A Maintenance Record for Security containers/Vault Doors (Optional Form 89), reference (b) Exhibit 10C, must be used as a permanent record of all repairs and alterations, and retained with the container. An annual inspection of the container will be performed and recorded by a qualified individual to verify the integrity of the container.

g. In mobile situations, TOP SECRET, SECRET, and/or CONFIDENTIAL keying material may be stored in a standard, approved field safe **or** in any similar security container secured by an electro-mechanical lock meeting Federal Specifications FF-L-2740.

h. Unclassified, unkeyed EKMS equipment may be stored in a manner sufficient to preclude any reasonable chance of

pilferage, theft, sabotage, tampering, or access by unauthorized persons.

i. Keyed equipment shall be protected to the level required by the highest classification of the equipment or the keying material. Additionally, procedures must be able to prevent unauthorized use or key extraction. When equipment containing encrypted key is located in an unmanned space, the Crypto Ignition Key (CIK) must be removed and protected in another location.

j. Fill devices (FD) containing unencrypted key marked or designated CRYPTO must be provided protection based on the highest classification of the key stored within.

k. Keyed Data Encryption System (DES) equipment and key loaders will be controlled and protected in the most secure manner available to the user. Unkeyed DES equipment and key loaders will be controlled and protected as highly valued property and should not be released to foreign nationals without prior approval from the National Security Agency (NSA) "I1" department.

12. Transporting EKMS Material

a. Commanding Officers, Officers-in-Charge, or Staff CMS Responsibility Officers are authorized in cases of operational necessity to approve the use of commercial aircraft to transport a quantity of EKMS material required to fulfill immediate, operational needs, **provided:**

(1) FAA Advisory Circular (AC NO, 108-3) and Departmental procedures are followed.

(2) Couriers are designated in writing and briefed on their responsibilities. Written instructions for safeguarding the material entrusted to them must be provided. Courier responsibilities are further delineated in Article 530f or reference (a), and Article 9-13 or reference (b).

b. Direct flights should be used. Transportation of keying material in aircraft flying over hostile territory should be avoided unless operationally necessary.

c. U.S. flag aircraft can be used to courier EKMS material within CONUS to include Alaska, Hawaii, and U.S. territories or possessions.

d. Transportation of EKMS material outside of CONUS on a U.S. flag, foreign-owned, or chartered aircraft is strongly discouraged.

e. EKMS material being transported within a command must be restricted to E-5 and above (or equivalent) personnel.

f. Private or corporate-owned conveyances can be used to carry EKMS material. The receiving organization should be notified of the itinerary and estimated time of arrival, so appropriate steps may be taken if the courier does not arrive on time.

g. CCI must not be shipped or transported in a keyed condition unless removing the key is impossible. CCI may be shipped or transported by any means delineated in Articles 535j through 535l of reference (a).

13. Routine Destruction of EKMS Material. Effective and superseded keying material is extremely sensitive and if compromised, potentially compromises all the information encrypted by it. For this reason, keying material must be properly and completely destroyed as soon as possible after it has been superseded or has otherwise served its intended purpose. Failure to destroy EKMS material within prescribed timeframes is a locally reportable Practice Dangerous to Security (PDS). A written report will be made to the CNRSW Staff EKMS Responsibility Officer (N60), per Chapter 10 of reference (a).

a. EKMS material authorized for destruction must always be destroyed and accurately documented by two properly cleared and authorized individuals.

b. Superseded keying material must be destroyed immediately after use when more than one copy of the key setting is available, or as soon as possible after the crypto period, but always within 12 hours after the end of the crypto period. Exceptions to the 12-hour destruction standard are outlined in Article 540e of reference (a).

(1) Superseded keying material on board aircraft is exempt from the 12-hour destruction standard; however, the material must be destroyed as soon as practicable upon completion of air operations.

(2) In the case of an extended holiday period (over 72 hours) or when special circumstances prevent compliance with the 12-hours destruction standard e.g., destruction facility or operational space not occupied, destruction may be extended until the next duty day. In such cases, the material must be destroyed as soon as possible after reporting for duty.

(3) LEs need not open security containers for the sole purpose of performing routine destruction of superseded segments; however, if the security containers are opened for any reason, all unsealed superseded material must be destroyed immediately.

c. A Segmental Destruction Form (CMS-25) will be maintained for all multi-copy/multi-segment EKMS keying material issued in non-electronic form. CMS-25 forms may be obtained from the EKMS Manager. Procedures for maintaining them are delineated in reference (a), Article 790.

d. A preprinted SF153 destruction report will be provided by the EKMS Manager with each routine issue of EKMS material. LEs shall, upon completion of destruction, sign, date, and obtain the Commanding Officer's, Officer-in-Charge's, or Staff EKMS Responsibility Officer's signature on the preprinted form and return it to the EKMS Manager no later than close of business on the second working day of the month. Retyped or substituted forms for the preprinted destruction report are not acceptable or authorized.

e. Destruction of keys issued to a Data Transfer Device (DTD) is accomplished by deletion. DTD audit trail reviews will serve to verify destruction of this key. Audit trail reviews must be accomplished by the LE Issuing personnel and the destruction reported to the parent account EKMS Manager on a Standard Form 153 (SF 153). The SF 153 will be dated and signed by the two personnel reviewing the DTD audit trail and the LE Commanding Officer. Upon request, the EKMS Manager can convert the DTD audit trail to a printed form.

f. Paper EKMS material shall be destroyed by burning, crosscut (double-cut) shredding, pulping, chopping, or pulverizing. Placing superseded material in a burn bag is not authorized.

(1) When burning, ensure the destruction is complete, no material has escaped, and all material has been reduced to white ash. Placing superseded keying material in a burn bag does not constitute a complete destruction. A complete destruction is the actual destruction by burning, shredding, or other authorized means that makes recovery or reproduction impossible.

(2) Shredding/Disintegration. Only paper material is authorized for shredding. Paper material that is shredded must be no larger than 5 mm. Key tape must be destroyed by burning or disintegration. If a disintegrator is not

available, key tape may be shredded and the residue burned. Maintain a record of material shredded/disintegrated while conducting destruction. The shredded/disintegrated material must be checked periodically during the destruction process to ensure complete destruction. Crosscut shredders must reduce the residue to shreds no more than 3/64-inch (1.2mm) by 1/2-inch (13mm) or 1/35-inch (0.73mm) by 7/8 inch (22.2mm). When destroying small amounts of keying material add an equal amount of other classified or unclassified material of similar composition before shredding.

g. Destruction by shredding is not considered sufficient to ensure complete destruction of diskettes. When diskettes containing keying material become superseded they must be returned to the EKMS Manager for disposition and documented on an SF 153 form or disintegrated by use of an authorized NSA-approved destruction device.

h. When an LE is underway or deployed, destruction will be conducted as normal and reported to the parent account EKMS Manager. The report may be a message identifying the two individuals conducting destruction, the date of destruction, and the material destroyed by short title, edition, and serial number. The EKMS Manager must receive the report by close of business on the second working day of the month. A signed copy of the destruction SF 153 form must be forwarded to the EKMS Manager. Delivery by facsimile, email, or U.S. mail is authorized.

14. Classification guidance. The following items must be classified at a minimum of CONFIDENTIAL:

a. Reports listing two-person-control (TPC) material.

b. Reports containing a complete record of classified keying material.

c. Reports indicating the effective date of classified keying material.

d. Classification must be determined by evaluating the content of each report or file and is the responsibility of the EKMS Manager(s) and the LE Issuing personnel. Consult Chapter 4 of reference (b) for further guidance.

15. Inventories. The Navy established the Fixed-Cycle inventory to ensure all accounts satisfy the national requirement for a semi-annual inventory of keying material. Commander, Navy Region Southwest has been assigned January and July to perform their semi-annual inventory. The EKMS Manager

prepares and distributes an inventory to each LE one-month prior to ensure ample time for reconciliation and reporting to the Central Office of Record (COR). All inventories must be conducted by the LE Issuing person with a qualified witness.

a. LEs shall conduct an inventory of all EKMS and STU-III material upon change of custodian, change of Commanding Officer, and semi-annual fixed-cycle inventory. If a change of custodian or change of command occurs during the semi-annual inventory, the inventories may be combined.

b. If EKMS material is deployed during an inventory, the LE shall obtain a message inventory report of all EKMS material held by the deployed detachments.

c. A change of custodian inventory must be conducted by the outgoing custodian and witnessed by the incoming custodian.

d. When conducting a semi-annual inventory, only inventory material up to and including the date preprinted on the inventory forms is provided by the EKMS Manager. Additions and deletions need not be recorded if they occurred after this date. All inventories require three signatures: the individual conducting the inventory, a qualified witness, and the Commanding Officer. Change of command inventories must be signed by the Commanding Officer being relieved. The signature of the Commanding Officer assuming command is optional.

e. LEs will maintain a current Accountable Item (AI) Summary (formerly called Running Inventory) of all EKMS material charged to their account. This includes, but is not limited to, physical keying material, electronic keying material stored in a common fill device or DTD, equipment, and manuals.

f. All EKMS material, including electronic key stored in a DTD, will be inventoried. Individuals conducting an inventory must sight the short title, edition suffix, and (if applicable) accounting number of each item of Accountability Legend Code (ALC) 1, 2, 4, 6, and 7 EKMS material held by the command. ALCs are defined in Annex A of reference (a).

g. In a watch station environment, all EKMS material must be inventoried on a watch-to-watch basis. The oncoming and outgoing watch supervisors shall personally sight each short title, edition, and accounting number. While on duty, each watch supervisor is responsible for all EKMS material listed on the watch-to-watch inventory. Watch station environment is defined in Article 775 of reference (a).

h. Unsealed EKMS materials, manuals, and classified components of issued repair or Q-kits must be page checked during every inventory.

16. Issuing EKMS Material. The EKMS Manager is responsible for the proper movement, internally or externally, of all EKMS material held by their account; therefore, all EKMS material movement within the CNRSW EKMS account will be coordinated with the EKMS Manager. EKMS material will be issued for use only after determining the intended recipients are properly cleared and authorized to hold/use EKMS material. The issue of EKMS material must be documented in order to maintain an audit trail for accountability purposes in the event the status of the material changes, e.g., supersession, compromise etc.

a. All personnel receiving EKMS material must be provided written instructions for properly safeguarding, handling, and accounting for EKMS material.

b. Every person issued EKMS material must complete a COMSEC Responsibility Acknowledgement Form prior to receiving the material. Authorized users of the Tactical Aircraft Mission Planning System (TAMPS) who are not directly issued GPS key, need not complete the COMSEC Responsibility Acknowledgement Form, but must hold a SECRET clearance.

c. Local custody is the acceptance of responsibility for the proper handling, safeguarding, accounting, and disposition of EKMS material issued by EKMS Manager and LE personnel.

d. CNRSW EKMS account uses the SF 153 (or a locally prepared equivalent approved by the EKMS Manager for issue, local custody, destruction, material returns, and inventories) for all accounting transactions. The minimum information required on each transaction is:

(1) From command.

(2) To command.

(3) Date of transaction.

(4) Short title, edition suffix, quantity, account number, and AL code(s) of material involved.

(5) Signature(s).

e. The issuing element must retain the original copy of the signed and dated local custody document and provide a copy

to the individuals receipting for the material. **A signed local custody form indicates assumption of responsibility for the material listed.**

f. CNRSW EKMS Manager requires two individuals, properly cleared and authorized by the Commanding Officer to receipt for material from CNRSW parent account. EKMS material will not be issued to a single individual.

g. CNRSW EKMS Manager assigns dates for routine issue of keying material. This is generally the last two weeks of each month. Although the issue is not restricted to these dates, LEs are strongly encouraged to make routine draw of keying material during normally assigned dates.

h. CNRSW issues keying material in a sealed package. The package contains a copy of the issue document (SF 153), a prepared document (SF 153) for material requiring destruction, the issued keying material, and any other useful information deemed appropriate at the time. The keying material will be inventoried and page checked, and the issue document signed and dated prior to leaving the CNRSW EKMS vault. LE personnel shall bring a lockable briefcase to receive the sealed package. Once LE personnel return to their command, they must open the package, inventory the contents and properly store the material.

i. Keying material marked or designated CRYPTO in hard copy form, may not be issued any earlier than 30 days prior to the effective period of the material. Authorization to exceed the 30-day issue timeframe during normal peacetime operations must be obtained from DCMS (N5).

j. Mobile users are authorized issue of a sufficient quantity of keying material to support mission requirements. This includes Marine Tactical units, SPECWAR units, NCB units, MIUW units, EOD units, and all aircraft.

k. When electronic key is issued in a common FD, recipients must acknowledge receipt of the key by signing local custody documents. Further distribution of the key (e.g., fill equipment, transfer to another FD, Over the Air Rekey (OTAR) of a circuit, or Over the Air Transfer (OTAT)) shall be recorded on an OTAT/OTAR form, found in Annexes P and Q of reference (a).

l. If keying material is issued via an FD, loading of the FD and issue to the LE will occur just before the planned mission. If a DTD is used, loading of encrypted key may occur 24 hours prior to the planned mission. When effective key remains stored in an FD following completion of a mission, the

device must be zeroized by LE personnel before returning the FD to the issuing element. Issuing elements must ensure FDs are zeroized immediately upon their return. LE custodians returning an FD to the parent account shall ensure the device has been zeroized whether the key is effective or not.

m. LE custodians are also required to conduct a monthly DTD audit and log the results. A copy of the Audit Trail Log must be hand-delivered or faxed to the parent account EKMS Manager by close of business on the second working of the each month. The Audit Trail Log shall be retained for two years. The LE Custodian has the option of bringing the DTD to the parent account for a printout of the audit trail or reviewing it themselves. Not reviewing the audit trail and recording the results are incidents, and an Incident Report will be filed per Chapter 9 of reference (a) LEs that do not comply **will not** be allowed to draw equipment or keying material, and an official notice of non-compliance will be forwarded to the LE's Commanding Officer. Enclosure (3) provides an example of a filled-in DTD Audit Trail Review Log.

n. Issuing elements are authorized to prematurely extract paper key from its protective packaging for the purpose of downloading the key in electronic form to an FD. The intentional removal must be recorded on the Destruction Record for Segmental Material (CMS 25) for the material, and the segments resealed per procedures outlined in Article 772 of reference (a).

o. Electronic key in an FD superseded during a mission must be zeroized within 12 hours of supersession. Exceptions to the 12-hour destruction standard are outlined in Article 540e of reference (a).

p. Each location holding electronic key in an FD must properly safeguard and continuously account for the loaded FD by serial number until the key is zeroized, overwritten, or otherwise destroyed.

q. LEs are authorized to draw keying material from other EKMS accounts when deployed or on extended missions. It is the LEs responsibility to coordinate EKMS support with the host unit to ensure mission readiness. LEs are strongly encouraged to coordinate well in advance of deployment and to exchange letters of agreement with the host command to ensure complete and proper support.

17. Sealing EKMS Material. LE Issuing personnel are responsible for ensuring the keying material is properly sealed or resealed. Keying material discovered removed from

its protective packaging before its effective period without documentation certifying removal was intentional, must be reported as an EKMS incident per Chapter 9 of reference (a).

a. Unsealed EKMS material may be sealed or resealed under the following conditions:

(1) To avoid daily page checks and destruction of superseded segments that will not be used for a significant period of time (e.g., two or more days).

(2) When all segments in a canister are intentionally removed due to packaging or production defect.

(3) When a segment(s) of keying material is unintentionally removed from its protective packaging before its effective period. This unintentional removal must be recorded on the destruction record of the material. Removal of key is defined as segment(s) pulled out of the canister but not detached or segment(s) detached from the canister.

b. Loose segmented keying material of the same day's key, from multiple copies, or from the same short titles shall not be sealed in the same container or envelope.

c. Only future segments of key may be sealed. All segments superseded prior to the material seal date must be destroyed and recorded on the destruction document of the material. Do not place a partially completed Destruction Record for Segmental Material (CMS 25) INSIDE THE SEALED ENVELOPE.

d. Unsealed segmented material may be considered resealed when placed in a container (e.g., zip-lock bag or a binder with plastic document protector pages) which will reasonably prevent the segments from being lost or misused. Page check segmented material prior to placing it in an envelope.

e. When material sealed in its original productive wrapper or resealed per Article 772 of reference (a) is opened, the material must be page checked and all superseded segments must be removed and destroyed immediately. The destructions shall be recorded on the destruction record (CMS 25) of the material.

f. Sealing/resealing procedures are outlined in Article 772h of reference (a).

18. Amendments and Corrections: Amendments and corrections are permanent changes to EKMS and EKMS-related publications that incorporate up-to-date information. Actions based on

outdated or incorrect information have the potential to adversely impact operational missions and administrative procedures. Publication amendments and corrections must be entered by properly trained and authorized personnel.

a. Changing a publication on the basis of an apparent discrepancy is not authorized. Changes to publications may be entered only as authorized by the publication's originator.

b. DCMS publications (CMS-1A, EKMS 1, EKMS 1 SUPP 1, CMS-9, etc.) are published on-line. Amendments to these publications will be distributed when an updated publication is placed on-line. Paper copies and CD-ROM versions of publications will no longer be distributed. Publications may be downloaded from the "Library" section of the CNRSW Web-page: https://www.ritsc-psw.navy.mil/ekms/.

Contact the EKMS Manager to obtain passwords for downloading from the CNRSW, DCMS, or INFOSEC Web-pages.

c. LE Issuing personnel are responsible for ensuring all required publications contain the most current amendments.

d. All pen-and-ink corrections to EKMS and EKMS-related publications must be made using black ink. Each pen-and-ink correction must be identified in the margin, opposite their entry (e.g., Amend 2, correction to Amend 2, etc.).

e. The individual entering an amendment or correction to an amendment must sign and date the Record of Amendments (ROA) page of the publication certifying the change was entered. A second authorized and properly trained individual must then verify the amendment and initial the entry on the ROA.

f. The "Check List For Entering Amendments to Publications" in Figure 7-4 of reference (a) provides step-by-step procedures for entering amendments. Individuals entering and verifying amendments are strongly encouraged to use this checklist for each amendment entry.

19. Extracts and Reproduction of EKMS Material. Reproduction of EKMS material is considered the complete reproduction of an **entire** Code, Authenticator, Call Sign (CAC) publication, or keylist, regardless of the reproduction method. Reproduction of less than an entire copy of material is an extract.

a. Per Article 781 of reference (a), the Commanding Officer may authorize the reproduction of an entire edition of CAC material. This authorization takes precedence over any restrictions or prohibitions against reproducing copies that may be contained in the Handling Instructions (HI) or Letter of Promulgation (LOP) of the material.

b. When reproduced for local command use, the user must account for CAC(s) locally and safeguard per assigned classification. Do **not** report the reproduction to higher authority.

c. Except in emergency situations, LEs are not authorized to reproduce CACs or keylists for transfer to another command. In an emergency, the Commanding Officer can authorize reproduction or extracts of CAC and keylists for another command with after the fact reporting to Controlling Authority (CA), DCMS (N30), and CNRSW EKMS Manager.

d. The following CAC material may **not** be reproduced:

(1) A U.S., Allied, or NATO Nuclear Command and Control Material.

(2) AKAA 285, AMSA TC 2, AMSA TX 9000, AMSA 661, AMSA 622, AMSC E/D 640, USKAC 878, USKAC 879, USKAI 4, AND USKAI 5.

e. Further guidance on reproduction and extracts of CAC and keylist is outlined in Articles 781 and 784 of reference (a).

20. EKMS Incidents and Practices Dangerous to Security (PDS). Because of the role EKMS material plays in the cryptographic processes to protect and authenticate U.S. Government information transmitted electronically, every type of EKMS material is in some way accounted for and controlled. To counter the threat posed to secure communications by EKMS material mishandling, losses, or thefts, the National Security Agency (NSA) established the National COMSEC Incident reporting and Evaluation System (NCIRES). To be effective the NCIRES must receive prompt and clear information relating to the circumstances surrounding an incident.

a. A report of any incident must be made regardless of the judgment of the EKMS manager or his/her supervisor as to whether or not an incident or possible incident occurred. Disciplinary action should not be taken against individuals for reporting an EKMS incident unless the incident occurred as the result of willful or gross negligence by those individuals.

b. LEs shall notify the EKMS Manager of any EKMS incident or PDS immediately after becoming aware of them. The LE will report EKMS incidents via message as promptly and accurately as possible. Do not delay reporting while gathering information. Reports for keying material incidents will be addressed "Action" to the controlling authority of the affected material.

Reports of incidents involving COMSEC equipment will be addressed "Action" to DIRNSA FT GEORGE G MEADE MD//I01P3//. Include COMNAVREG SW SAN DIEGO CA//N6/N632// as an information addressee on all reports from Initial through Final.

c. Guidelines for identifying and reporting EKMS incidents are in Chapter 9 of reference (a).

d. PDSs, while not reportable to the national level (NSA), are practices that have the **potential** to jeopardize the security of the EKMS material **if** allowed to perpetuate.

e. All LEs must conduct annual PDS familiarization training which will, at a minimum, include a review and discussion of Article 1005 of reference (a). Provide a report of this training to the EKMS Manager within five days of completion.

f. There are only two PDSs reportable outside the EKMS account command and both incidents must be reported to the Controlling Authority (CA) of the keying material involved:

(1) Premature or out-of-sequence use of keying material before its effective date as long as the material was not reused. If the material was reused without the permission of the CA, it becomes a reportable EKMS incident.

(2) Inadvertent (early) destruction of EKMS material or destruction without authorization of the CA, but documented properly, is not a reportable incident. If the destruction was not properly documented, it becomes a reportable EKMS incident.

g. All other PDSs listed in Article 1005 of reference (a) will be reported to the EKMS Manager immediately after becoming known. The LE command will submit a letter report to CNRSW (N60) explaining the incident and identifying procedures to preclude recurrence. This letter will be retained in the Correspondence/Message file for two years.

21. Emergency Action Plan (EAP). Per Exhibit 2-B of reference (b), Commanding Officers shall develop an emergency plan for the protection of classified information in cases of natural disaster, terrorism, or civil disturbance. Commands located outside the U.S. and its territories and units that are deployable, require an emergency destruction supplement for their emergency plans. It is the responsibility of the LE Issuing Personnel to maintain the EKMS portion of the command EAP.

a. Every command that holds classified EKMS or CCI material must prepare emergency plans for safeguarding such material in the event of an emergency.

b. For commands located within the 48 contiguous states, planning must consider natural disasters (e.g., fire, flood, tornado, and earthquake), civil/mob actions, and terrorism when developing their plan. For all other commands and deployable units, planning must consider both natural disasters and local hostile action to include enemy attack, terrorism, and mob actions.

c. Accurate information relative to the extent of an emergency is absolutely essential to the effective evaluation of the COMSEC impact of the occurrence, and is second in importance only to the complete and thorough destruction itself.

d. The senior official shall report the facts surrounding the destruction to CNO WASHINGTON DC//N614//, CNI WASHINGTON DC//N6//, COMNAVNETWARCOM NORFOLK VA//N6//, COMNAVNETSPAOPSCOM DAHLGREN VA//N6//, DCMS WASHINGTON DC//N5//, DIRNSA FT GEORGE G MEADE MD//I01P3/I513//, and both operational and administrative chains-of-command as soon as possible. If feasible, use a secure means of reporting.

e. Complete guidance for developing an EAP is located in Annex L of reference (a).

N. YOUNG-ARANITA
By direction

DEC 0 1 2004

[Letter Head]

2280
N1
Date

From: *(Commanding Officer, Command Title)*
To: EKMS Manager, Navy Region Southwest

Subj: AUTHORIZATION TO RECEIPT FOR AND COURIER COMSEC MATERIAL

Ref: (a) CMS 21
(b) COMNAVREGSWINST 2280.1A

1. Per references (a) and (b), the below named individuals are authorized to receipt for and courier COMSEC material for this command.

Rank/Rate/ Grade	NAME *(last, first, MI)*	SSN *(Last 4)*	CLEARANCE	POSITION *(Custodian/ Alternate)*
a.				
b.				
c.				
d.				

2. _____

a. EKMS ID Number: 151016

b. *(Highest classification Indicator)* HCI: _____

c. Command Telephone Number(s): COMM: (____) _____
DSN: _____
FAX: _____

d. Custodian E-Mail Address: _____

e. ISIC: _____

3. I certify that the individuals identified above are assigned to my command, are authorized and possess a security clearance equal to or higher than that of the COMSEC material being handled.

[signature]

Enclosure (1)

COMNAVREGSWINST 2280.1A

DEC 0 1 2004

CMS 21B

TAB-6 TO ANNEX AF TO CMS 21B

CRYPTO IGNITION KEY (CIK) DATA LOG

COMMAND_COMNAVREG SW
ACCOUNT NUMBER_151016___

USE OF THESE BLOCKS OPTIONAL

ID OF KEY ASSOCIATED WITH CIK USKAU 1005	STU-III SER NO IN WHICH KEY IS LOADED	WHERE TERMINAL IS INSTALLED (BLDG/ROOMNUMBER)	DATE CIK CREATED OR DATE TERMINAL KEYED	CIK SERIAL NO	M-MASTER U-USER	CIK SEQUENCE OF 8 ETC	ID OF CIK USER	PHONE # OF CIK USER	DATE CIK DELETED OR ZEROIZED	DISPOSITION/ REMARKS	DATE	SIGNATURE OF CUSTODIAN
1234567	2375	B318 R118	09/18/04	EEAA-1234	M	1	CO	5/1234				
1234567	25912	B112 R205	09/18/04	EAKB-2233	U	2	CO	5/1234				

PAGE_____OF_____

Enclosure (2)

DEC 0 1 2004

DTD
AUDIT TRAIL REVIEW LOG
(REVIEWS TO BE COMPLETED AT
30 DAY INTERVALS OR LESS)

DTD SERIAL NUMBER:	**_172536**		**ISSUED**
ASSOCIATED CIKS:	**_3_(QTY)**		**YES/NO**
CIK SERIAL NUMBER:	**253601**	**(SUPERVISORY)**	**N**
	253603	**(USER)**	**Y**
	253604	**(USER)**	**Y**

REVIEW DATE	CIK NUMBER	DTDISSUE DATE	TURN IN DATE	REMARKS(I.E.: AUDIT TRAIL RVW/CLEARED/COMMENTS)	RVW/ BY
07/30/04	253601	N/A	N/A	NO ANOMOLIES / RESET	J. SALTY
08/31/04	253601	N/A	N/A	NO ANOMOLIES / RESET	J. SALTY

CMS-21, ANNEX AC
RETAIN LOG FOR 2 YEARS